



UNITED STATES PATENT AND TRADEMARK OFFICE

mn

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,391	10/07/2003	Jong-Su Lim	44824	5463

7590 06/26/2007
Peter L. Kendall
Roylance, Abrams, Berdo & Goodman, L.L.P.
Suite 600
1300 19th Street, N.W.
Washington, DC 20036

EXAMINER

DEBNATH, SUMAN

ART UNIT	PAPER NUMBER
----------	--------------

2135

MAIL DATE	DELIVERY MODE
-----------	---------------

06/26/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/679,391	LIM, JONG-SU	
	Examiner	Art Unit	
	Suman Debnath	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 March 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 28 March 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-12 are pending in this application.
2. Claims 1-2, 4-5 and 8 are presently amended in the amendment filed 28 March 2007.
3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

Claim Objections

4. Claims 2 and 3 are objected to because of the following informalities:

Claim 2 recites "**second encryption code** comprises at least one of **KO.sub.1,1**, KO.sub.1,2, KO.sub.1,3, KI.sub.1,1, KI.sub.1,2, and KI.sub.1,3" in line 1. However, claim 4 recites "KO.sub.1,1" as "the **first** encryption code" in line 4. Examiner will treat the limitation of claim 2 as "first encryption code" for the purpose of examination.

Claim 3 recites "the **first** predetermined encryption codes comprises at least one of **KO.sub.2,1**, KO.sub.2,2, KO.sub.2,3, KI.sub.2,1, KI.sub.2,2, and KI.sub.2,3" in line 1. However, claim 5 recites "KO.sub.2,1" as "the **second** encryption code" in line 4. Examiner will treat the limitation of claim 3 as "the **second** predetermined encryption codes" for the purpose of examination.

Appropriate correction and/or clarification is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-5 and 7-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's admitted prior art, hereinafter "AAPA," and in view of 3rd Generation Partnership Project, "Document 2: KASUMI Specification" Release 4, 2001-08-28, hereinafter "DKS" and further in view of Hoffman (Patent No.: US 6,324,288 B1).

7. As to claim 1, AAPA discloses an encryption method for dividing a first plaintext bit stream of length $2n$ into first and second sub-bit streams of length n (FIG. 1, item 210, L.sub.01 is an input to FO1 unit which takes two sub-bit stream input, see FIG. 2B), dividing a second plaintext bit stream of length $2n$ into third and fourth sub-bit streams of length n (FIG. 1, item 220, input of FO2 takes two sub-bit stream), and generating a ciphertext bit stream of length $2n$ from the first, second, third and fourth sub-bit streams using 2-rounds of encryption (FIG. 1, item 210 and 220), the method comprising the steps of:

performing a first-round of encryption by encrypting the received first and second sub-bit streams with predetermined first encryption codes an odd number of times, and outputting a second ciphertext bit stream having been once more encrypted with a predetermined time delay after first ciphertext bit streams of length n are outputted (FIG.

2B, specification, page 3, lines 23-30 and page 4, lines 1-15; AAPA discloses a block diagram of FOi units which generates first and second ciphertext bit streams R.sub.4' and L.sub.4' after receiving the first sub-bit stream L.sub.0' and second sub-bit stream R.sub.0' with predetermined first encryption codes KO.sub.1,1, KO.sub.1,2, KO.sub.1,3, KI.sub.1,1, KI.sub.1,2, and KI.sub.1,3; Second ciphertext bit stream L.sub.4' being output with predetermined time delay, see e.g., FIG. 2B, item 50);

generating a first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first ciphertext bit stream and the third sub-bit stream (specification, page 2, lines 14-17, FIG. 1, which teaches output of FO1 unit performs an exclusive-OR operation with R.sub.0 to provide input for second FO2 unit);

generating a second operated ciphertext bit stream by performing a logical exclusive-OR operation on the second ciphertext bit stream and the fourth sub-bit stream (specification, page 2, lines 14-17, FIG. 1, , which teaches output of FO1 unit performs an exclusive-OR operation with R.sub.0 to provide input for second FO2 unit); and

performing a second-round of encryption by encrypting the received the first operated ciphertext bit stream (specification, page 2, lines 8-10, describes FOi units. "i" reads on second round, see e.g., FIG. 1, item 220 and FIG. 2B teaches the implementation of item 220, R.sub.4' reads on outputting the third ciphertext bit and L.sub.4' reads on outputting fourth ciphertext bit stream) and the second operated ciphertext bit stream having the predetermined time delay with predetermined encryption codes an odd number of times (FIG. 2B, L.sub.0' reads on first operated

ciphertext bit stream and R.sub.0' reads on second operated ciphertext bit stream; FIG. 1 teaches second round (item 220) that takes input from output of first round (item 210) combined with R.sub.0 by performing an exclusive-OR operation which causes time delay), and concurrently outputting the third and fourth ciphertext bit streams of length n after once more encrypting the first operated ciphertext bit stream with predetermined encryption codes (FIG. 2B, specification, page 3, lines 23-30 and page 4, lines 1-15).

AAPA doesn't explicitly disclose performing encryption of first and second ciphertext bit stream at the same time; and predetermined second encryption codes. However, using second set of predetermined encryption code for second round encryption is standard in Kasumi encryption algorithm as taught by DKS (page 12, section 4.3, which describes $KO.sub.i = KO.sub.i,1 \parallel KO.sub.i,2 \parallel KO.sub.i,3$ and $Kl.sub.i = Kl.sub.i,1 \parallel Kl.sub.i,2 \parallel Kl.sub.i,3$; "i" represents rounds, see e.g., page 10, section 2.3, line 10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of AAPA by using second set of predetermined encryption code for second round encryption as taught by DKS in order to increase the confidentiality and integrity of the encrypted data. Furthermore, one would be motivated to do so to transmit data over the public network.

Neither, AAPA nor DKS explicitly discloses performing encryption of first and second ciphertext bit stream at the same time. However, Hoffman discloses performing encryption of first and second ciphertext bit stream at the same time ("As soon as the second stage has started, the first stage begins encrypting the next block. In this

manner, the cipher core concurrently processes two blocks at a time resulting in throughput approaching twice that of a single stage implementation” –e.g. column 11, lines 60-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of AAPA and DKS as taught by Hoffman in order to “optimize speed” (Hoffman, column 11).

8. As to claim 2, AAPA discloses wherein the predetermined first encryption codes comprises at least one of KO.sub.1,1, KO.sub.1,2, KO.sub.1,3, KI.sub.1,1, KI.sub.1,2, and KI.sub.1,3 (specification, page 2, lines 26-30 and page 3, lines 2-11).

9. As to claim 3, DKS discloses the second predetermined encryption codes comprises at least one of KO.sub.2,1, KO.sub.2,2, KO.sub.2,3, KI.sub.2,1, KI.sub.2,2, and KI.sub.2,3 (specification, page 12, section 4.3, which describes $KO.sub.i = KO.sub.i,1 \parallel KO.sub.i,2 \parallel KO.sub.i,3$ and $KI.sub.i = KI.sub.i,1 \parallel KI.sub.i,2 \parallel KI.sub.i,3$, “i” reads on 2, see e.g., page 10, section 2.3, line 10).

10. As to claim 4, AAPA discloses the first-round encryption (FIG. 1, item 210) step comprises the steps of:

generating a first signal by performing a logical exclusive-OR operation on the first sub-bit stream and the first encryption code KO.sub.1,1 to provide a first exclusive-OR operated bitstream (specification, page 3, lines 26-29), encrypting the first

exclusive-OR-operated bit stream with the first encryption code Kl.sub.1,1 to provide a first encrypted signal (specification, page 3, lines 29-30), and performing a logical exclusive-OR operation on the first encrypted signal and the second sub-bit stream (specification, page 4, lines 2-3), delayed by time required for the encryption (specification, page 4, line 1);

generating the first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second sub-bit stream and the first encryption code KO.sub.1,2 (specification, page 4, lines 3-5), to provide a second exclusive-OR operated bitstream encrypting the second exclusive-OR-operated bit stream with the first encryption code Kl.sub.1,2, to provide a second encrypted signal (specification, page 4, lines 5-6), and performing a logical exclusive-OR-operation on the second encrypted signal and the first signal (specification, page 4, lines 7-8);

generating the second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first signal and the first encryption code KO.sub.1,3 to provide a third exclusive-OR operated bitstream (specification, page 4, lines 8-10), encrypting the third exclusive-OR-operated bit stream with the first encryption code Kl.sub.1,3 (specification, page 4, lines 10-11), and performing a logical exclusive-OR-operation on the encrypted signal with the first sub-bit stream delayed by time required for the encryption (specification, page 4, lines 11-14).

11. As to claim 5, AAPA discloses the second-round encryption (FIG. 1, item 220) step comprises the steps of:

generating a second signal by performing a logical exclusive-OR-operation the first operated ciphertext bit stream and the encryption code to provide a fourth exclusive-OR operated bitstream (specification, page 3, lines 26-29); encrypting the fourth exclusive-OR-operated bit stream with the encryption code to provide a third encrypted signal (specification, page 3, lines 29-30); performing a logical exclusive-OR-operation on the third encrypted signal and the second operated ciphertext bit stream to provide a fifth exclusive-OR operated bitstream (specification, page 4, lines 2-3);

generating the third ciphertext bit stream by performing a logical exclusive-OR-operation on the second operated ciphertext bit stream and the encryption code (specification, page 4, lines 3-5); encrypting the fifth exclusive-OR-operated bit stream with the encryption code to provide a fourth encrypted signal (specification, page 4, line 5-8); and performing a logical exclusive-OR-operation on the fifth encrypted signal and the second signal (specification, page 4, lines 9-10); delayed by time required for the encryption (specification, page 4, line 12); and

generating the fourth ciphertext bit stream by performing a logical exclusive-OR-operation on the second signal and the encryption code (specification, page 4, lines 7-10); encrypting the sixth exclusive-OR-operated bit stream with the encryption code (specification, page 4, lines 10-11); and performing a logical exclusive-OR-operation on the encrypted signal with the third ciphertext bit stream (specification, page 4, lines 11-14).

AAPA doesn't explicitly disclose performing the corresponding second-round encryption using predetermined second encryption codes KO.sub.2,1, KI.sub.2,1,

Art Unit: 2135

KO.sub.2,2, Kl.sub.2,2, KO.sub.2,3 and Kl.sub.2,3. However, using second set of predetermined encryption code for second round encryption is standard in Kasumi encryption algorithm as taught by DKS (page 12, section 4.3, which describes KO.sub.i=KO.sub.i,1 || KO.sub.i,2 || KO.sub.i,3 and Kl.sub.i= Kl.sub.i,1 || Kl.sub.i,2, || Kl.sub.i,3, "i" reads on 2, see e.g., page 10, section 2.3, line 10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of AAPA by using second set of predetermined encryption code for second round encryption as taught by DKS in order to increase the confidentiality and integrity of the encrypted data. Furthermore, one would be motivated to do so to transmit data over the public network.

12. As to claim 7, AAPA discloses the encryption method wherein a 16-bit input bit stream is divided into a 9-bit stream and a 7-bit stream (specification, page 4, lines 22-24, FIG. 3), a 9-bit ciphertext bit stream is generated from the 9-bit stream using a first equation (specification, page 4, lines 24-25), and a 7-bit ciphertext bit stream is generated from the 7-bit stream using a second equation in each of the sub-encryptions (speciation, page 5, line 12), wherein said first equation comprises

$$\begin{aligned}
 y_0 &= (x_0x_2) \oplus x_3 \oplus (x_2x_5) \oplus (x_5x_6) \oplus (x_0x_7) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (\\
 &x_4x_8) \oplus (x_5x_8) \oplus (x_7x_8)' \oplus 1'; y_1 = x_1 \oplus (x_0x_1) \oplus (x_2x_3) \oplus (x_0x_4) \oplus (x_1x_4) \oplus \\
 &(x_0x_5) \oplus (x_3x_5) \oplus x_6 \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_5x_8)' \oplus 1'; y_2 = x_1 \oplus (x_0x_3) \oplus (\\
 &x_3x_4) \oplus (x_0x_5) \oplus (x_2x_6) \oplus (x_3x_6) \oplus (x_5x_6) \oplus (x_4x_7) \oplus (x_5x_7) \oplus (x_6x_7) \oplus x_8 \oplus \\
 &(x_0x_8)' \oplus 1'; y_3 = x_0 \oplus (x_1x_2) \oplus (x_0x_3) \oplus (x_2x_4) \oplus x_5 \oplus (x_0x_6) \oplus (x_1x_6) \oplus (
 \end{aligned}$$

Art Unit: 2135

$x_4x_7) \oplus (x_0x_8) \oplus (x_1x_8) \oplus (x_7x_8); y_4 = (x_0x_1) \oplus (x_1x_3) \oplus x_4 \oplus (x_0x_5) \oplus (x_3x_6)$
 $\oplus (x_0x_7) \oplus (x_6x_7) \oplus (x_1x_8) \oplus (x_2x_8) \oplus (x_3x_8); y_5 = x_2 \oplus (x_1x_4) \oplus (x_4x_5) \oplus ($
 $x_0x_6) \oplus (x_1x_6) \oplus (x_3x_7) \oplus (x_4x_7) \oplus (x_6x_7) \oplus (x_5x_8) \oplus (x_6x_8) \oplus (x_7x_8)' \oplus 1';$
 $y_6 = x_0 \oplus (x_2x_3) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_4x_5) \oplus (x_3x_6) \oplus (x_4x_6) \oplus (x_5x_6) \oplus x_7$
 $\oplus (x_1x_8) \oplus (x_3x_8) \oplus (x_5x_8) \oplus (x_7x_8); y_7 = (x_0x_1) \oplus (x_0x_2) \oplus (x_1x_2) \oplus x_3 \oplus ($
 $x_0x_3) \oplus (x_2x_3) \oplus (x_4x_5) \oplus (x_2x_6) \oplus (x_3x_6) \oplus (x_2x_7) \oplus (x_5x_7) \oplus x_8' \oplus 1'; y_8 = ($
 $x_0x_1) \oplus x_2 \oplus (x_1x_2) \oplus (x_3x_4) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_1x_6) \oplus (x_4x_6) \oplus x_7 \oplus ($
 $x_2x_8) \oplus (x_3x_8)$ (specification, page 5, line 1, equation 1);

Second equation comprises $y_0 = (x_1x_3) \oplus x_4 \oplus (x_0x_1x_4) \oplus x_5 \oplus (x_2x_5) \oplus ($
 $x_3x_4x_5) \oplus x_6 \oplus (x_0x_6) \oplus (x_1x_6) \oplus (x_3x_6) \oplus (x_2x_4x_6) \oplus (x_1x_5x_6) \oplus (x_4x_5x_6); y$
 $_1 = (x_0x_1) \oplus (x_0x_4) \oplus (x_2x_4) \oplus x_5 \oplus (x_1x_2x_5) \oplus (x_0x_3x_5) \oplus x_6 \oplus (x_0x_2x_6) \oplus ($
 $x_3x_6) \oplus (x_4x_5x_6)' \oplus 1'; y_2 = x_0 \oplus (x_0x_3) \oplus (x_2x_3) \oplus (x_1x_2x_4) \oplus (x_0x_3x_4) \oplus ($
 $x_1x_5) \oplus (x_0x_2x_5) \oplus (x_0x_6) \oplus (x_0x_1x_6) \oplus (x_2x_6) \oplus (x_4x_6)' \oplus 1'; y_3 = x_1 \oplus ($
 $x_0x_1x_2) \oplus (x_1x_4) \oplus (x_3x_4) \oplus (x_0x_5) \oplus (x_0x_1x_5) \oplus (x_2x_3x_5) \oplus (x_1x_4x_5) \oplus (x_2x_6$
 $) \oplus (x_1x_3x_6); y_4 = (x_0x_2) \oplus x_3 \oplus (x_1x_3) \oplus (x_1x_4) \oplus (x_0x_1x_4) \oplus (x_2x_3x_4) \oplus ($
 $x_0x_5) \oplus (x_1x_3x_5) \oplus (x_0x_4x_5) \oplus (x_1x_6) \oplus (x_3x_6) \oplus (x_0x_3x_6) \oplus (x_5x_6)' \oplus 1'; y_5$
 $= x_2 \oplus (x_0x_2) \oplus (x_0x_3) \oplus (x_1x_2x_3) \oplus (x_0x_2x_4) \oplus (x_0x_5) \oplus (x_2x_5) \oplus (x_4x_5) \oplus ($
 $x_1x_6) \oplus (x_1x_2x_6) \oplus (x_0x_3x_6) \oplus (x_3x_4x_6) \oplus (x_2x_5x_6)' \oplus 1'; y_6 = (x_1x_2) \oplus ($
 $x_0x_1x_3) \oplus (x_0x_4) \oplus (x_1x_5) \oplus (x_3x_5) \oplus x_6 \oplus (x_0x_1x_6) \oplus (x_2x_3x_6) \oplus (x_1x_4x_6) \oplus ($
 $x_0x_5x_6)$ (specification, page 5, line 15, equation 2);

13. As to claim 8, AAPA discloses an encryption apparatus for dividing a first plaintext bit stream of length $2n$ into first and second sub-bit streams of length n (FIG. 1, item 210, L.sub.01 is an input to FO1 unit which takes two sub-bit stream input, see FIG. 2B), dividing a second plaintext bit stream of length $2n$ into third and fourth sub-bit streams of length n (FIG. 1, item 220, input of FO2 takes two sub-bit stream), and generating a ciphertext bit stream of length $2n$ from the first, second, third and fourth sub-bit streams using 2-rounds of encryption (FIG. 1, item 210 and 220 provides 2-rounds of encryption), the apparatus comprising:

a first ciphering unit (FIG. 1, item 210) for receiving the first and second sub-bit streams (specification, page 3, lines 26-27, L.sub.0' reads on the first sub-bit stream and R.sub.0' reads second sub-bit stream), and generating first and second ciphertext bit streams of length n by encrypting the first and second sub-bit streams with predetermined first encryption codes KO.sub.1,1, KO.sub.1,2, KO.sub.1,3, KI.sub.1,1, KI.sub.1,2, and KI.sub.1,3 an odd number of times, and the second ciphertext bit stream having been once more encrypted with a predetermined time delay after the first ciphertext bit streams of length n are outputted. (FIG. 2B, specification, page 3, lines 23-30 and page 4, lines 1-15; AAPA discloses a block diagram of FOi units which generates first and second ciphertext bit streams R.sub.4' and L.sub.4' after receiving the first sub-bit stream L.sub.0' and second sub-bit stream R.sub.0' with predetermined first encryption codes KO.sub.1,1, KO.sub.1,2, KO.sub.1,3, KI.sub.1,1, KI.sub.1,2, and KI.sub.1,3; Second ciphertext bit stream L.sub.4' being output with predetermined time delay, see e.g., FIG. 2B, item 50);

an operating unit for generating a first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first ciphertext bit stream and the third sub-bit stream (specification, page 2, lines 14-17, FIG. 1, which teaches output of FO1 unit performs an exclusive-OR operation with R.sub.0 to provide input for second FO2 unit), and generating a second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second ciphertext bit stream with the fourth sub-bit stream (specification, page 2, lines 14-17, FIG. 1, which teaches output of FO1 unit performs an exclusive-OR operation with R.sub.0 to provide input for second FO2 unit); and

a second ciphering unit (FIG. 1, item 220) for receiving the first operated ciphertext bit stream and the second operated ciphertext bit stream having the predetermined time delay (FIG. 2B, L.sub.0' reads on first operated ciphertext bit stream and R.sub.0' reads on second operated ciphertext bit stream; FIG. 1 teaches second round (item 220) that takes input from output of first round (item 210) combined with R.sub.0 by performing an exclusive-OR operation which causes time delay), generating third and fourth ciphertext bit streams of length n by encrypting the first operated ciphertext bit stream and the second operated ciphertext bit stream with predetermined encryption codes an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams after once more encrypting the first operated ciphertext bit stream with predetermined encryption codes (FIG. 2B, specification, page 3, lines 23-30 and page 4, lines 1-15; R.sub.4' reads on the third ciphertext bit and L.sub.4' reads on

fourth ciphertext bit stream) and concurrently outputting the third and fourth ciphertext bit streams (specification, page 4, lines 12-15).

AAPA doesn't explicitly disclose at the same time of performing first and second round of encryption; and the use of predetermined second encryption codes KO.sub.2,1, KI.sub.2,1, KO.sub.2,2, KI.sub.2,2, KO.sub.2,3 and KI.sub.2,3.

However, using second set of predetermined encryption code for second round encryption is standard in Kasumi encryption algorithm as taught by DKS (page 12, section 4.3, which describes $KO.sub.i = KO.sub.i,1 \parallel KO.sub.i,2 \parallel KO.sub.i,3$ and $KI.sub.i = KI.sub.i,1 \parallel KI.sub.i,2 \parallel KI.sub.i,3$, "i" reads on 2, see e.g., page 10, section 2.3, line 10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of AAPA by using second set of predetermined encryption code for second round encryption as taught by DKS in order to increase the confidentiality and integrity of the encrypted data. Furthermore, one would be motivated to do so to transmit data over the public network.

Neither AAPA nor DKS explicitly disclose at the same time of performing first and second round of encryption. However, Hoffman discloses at the same time of performing first and second round of encryption ("As soon as the second stage has started, the first stage begins encrypting the next block. In this manner, the cipher core concurrently processes two blocks at a time resulting in throughput approaching twice that of a single stage implementation" —e.g. column 11, lines 60-65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of AAPA and DKS as taught by Hoffman in order to "optimize speed" (Hoffman, column 11).

14. As to claim 9, AAPA discloses the encryption apparatus wherein the first ciphering unit (FIG. 1, item 210) comprises:

a first block having a first exclusive-OR operator for performing a logical exclusive-OR operation on the first sub-bit stream and the first encryption code KO.sub.1,1 (specification, page 3, lines 26-29), a first sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code KI.sub.1,1 (specification, page 3, lines 26-29), and a second exclusive-OR operator for generating a first signal by performing a logical exclusive-OR operation on the encrypted signal with the second sub-bit stream being delayed to provide time for the encryption (specification, page 4, lines 1-3);

a second block having a third exclusive-OR operator for performing a logical exclusive-OR operation on the second sub-bit stream and the first encryption code KO.sub.1,2 (specification, page 4, lines 3-5), a second sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code KI.sub.1,2 (specification, page 4, lines 4-5), and a fourth exclusive-OR operator for generating the first operated ciphertext bit stream by performing a logical exclusive-OR operation on the encrypted signal and the first signal (specification, page 4, lines 7-8); and a third block having a fifth exclusive-OR operator for performing a logical exclusive-OR

operation on the first signal and the first encryption code KO.sub.1,3 (specification, page 4, lines 8-10),

a third sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code KI.sub.1,3 (specification, page 4, line 10-11), and a sixth exclusive-OR operator for generating the second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the encrypted signal and the first sub-bit stream delayed by time required for the encryption (specification, page 4, lines 11-14).

15. As to claim 10, AAPA discloses the encryption apparatus wherein the second ciphering unit (FIG.1, item 220) comprises:

a fourth block having a seventh exclusive-OR operator for exclusive-OR-operating the first operated ciphertext bit stream with the encryption code (specification, page 3, lines 26-29), a fourth sub-cipher for encrypting the exclusive-OR-operated bit stream with the encryption code (specification, page 3, lines 29-30), and an eighth exclusive-OR operator for generating a second signal by performing a logical exclusive-OR-operation on the encrypted signal and the second operated ciphertext bit stream (specification, page 4, lines 2-3);

a fifth block having a ninth exclusive-OR operator for exclusive-OR-operating the second operated ciphertext bit stream with the encryption code (specification, page 4, lines 3-5), a fifth sub-cipher for encrypting the exclusive-OR-operated bit stream with the encryption code (specification, page 4, line 5-6), and a tenth exclusive-OR operator for generating the third ciphertext bit stream by performing a logical exclusive-OR-operation

on the encrypted signal (specification, page 4, line 5-8) and the second signal delayed by time required for the encryption (specification, page 4, line 8); and a sixth block having an eleventh exclusive-OR operator for performing a logical exclusive-OR operation on the second signal with the encryption code (specification, page 4, lines 8-10),

a sixth sub-cipher for encrypting the exclusive-OR-operated bit stream with the encryption code (specification, page 4, lines 10-11), and a twelfth exclusive-OR operator for generating the fourth ciphertext bit stream by performing a logical exclusive-OR operation on the encrypted signal and the third ciphertext bit stream (specification, page 4, lines 11-14).

AAPA doesn't explicitly disclose the use of second-round encryption using predetermined second encryption codes KO.sub.2,1, KI.sub.2,1, KO.sub.2,2, KI.sub.2,2, KO.sub.2,3 and KI.sub.2,3. However, using second set of predetermined encryption code for second round encryption is standard in Kasumi encryption algorithm as taught by DKS (page 12, section 4.3, which describes $KO.sub.i = KO.sub.i,1 \parallel KO.sub.i,2 \parallel KO.sub.i,3$ and $KI.sub.i = KI.sub.i,1 \parallel KI.sub.i,2 \parallel KI.sub.i,3$, "i" reads on 2, see e.g., page 10, section 2.3, line 10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of AAPA by using second set of predetermined encryption code for second round encryption as taught by DKS in order to increase the confidentiality and integrity of the encrypted data. Furthermore, one would be motivated to do so to transmit data over the public network.

16. Claims 6 and 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA and further in view of DKS, Hoffman and Campbell, Jr. (Patent No.: 4,304,961), hereinafter "Campbell".

17. As to claim 6, AAPA discloses each of the encryptions includes first and second sub-encryptions (FIG. 3, items S91, S71 reads on first sub-encryption and items S92, S72 reads on second sub-encryption).

Neither AAPA and DKS nor Hoffman explicitly discloses the outputs from the first and second sub-encryptions are stored and simultaneously retrieved according to an external clock signal. However, Campbell discloses the outputs are stored and simultaneously retrieved according to an external clock signal (FIG. 1A, items 18, 20, 22, FIG. 2; column 5, lines 66-68 and column 6, lines 1-7 and 11-16).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of AAPA, DKS and Hoffman by storing the outputs from the first and second sub-encryptions and simultaneously retrieving according to an external clock signal as taught by Campbell in order to "provide and improved authenticator code generator for generating a unique authenticator code which is dependent on a key variable stored in the authenticator code generator and the text of a received message" (Campbell, column 3, lines 45-49).

18. As to claim 11, AAPA discloses each of the first to sixth sub-ciphers (FIG 1. items 210 and 220 each has three sub-ciphers, e.g., see FIG. 2A and FIG. 2B) includes first and second sub-ciphering units (FIG. 3, items S91, S71 reads on first sub-encryption and items S92, S72 reads on second sub-encryption).

Neither AAPA and DKS nor Hoffman explicitly discloses a register for storing the outputs of the first and second sub-ciphering units and simultaneously retrieve the outputs according to an external clock signal. However, Campbell discloses a register for storing the outputs and simultaneously retrieves the outputs according to an external clock signal (FIG. 1A, items 18, 20, 22, FIG. 2; column 5, lines 66-68 and column 6, lines 1-7 and 11-16).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of AAPA, DKS and Hoffman by storing the outputs from the first and second sub-encryptions and simultaneously retrieving according to an external clock signal as taught by Campbell in order to "provide and improved authenticator code generator for generating a unique authenticator code which is dependent on a key variable stored in the authenticator code generator and the text of a received message" (Campbell, column 3, lines 45-49).

19. As to claim 12, AAPA discloses the encryption apparatus wherein each of the first and second sub-ciphering units divides a 16-bit input bit stream into a 9-bit stream and a 7-bit stream (specification, page 4, lines 22-24, FIG. 3), and generates a 9-bit ciphertext bit stream from the 9-bit stream using a third equation (specification, page 4,

Art Unit: 2135

lines 24-25), and a 7-bit ciphertext bit stream from the 7-bit stream using a fourth equation (specification, page 5, line 12), said third equation comprising

$$\begin{aligned}
 y_0 = & (x_0x_2) \oplus x_3 \oplus (x_2x_5) \oplus (x_5x_6) \oplus (x_0x_7) \oplus (x_1x_7) \oplus (x_2x_7) \oplus (\\
 & x_4x_8) \oplus (x_5x_8) \oplus (x_7x_8)' \oplus 1'; y_1 = x_1 \oplus (x_0x_1) \oplus (x_2x_3) \oplus (x_0x_4) \oplus (x_1x_4) \oplus \\
 & (x_0x_5) \oplus (x_3x_5) \oplus x_6 \oplus (x_1x_7) \oplus (x_2x_7) \oplus (x_5x_8)' \oplus 1'; y_2 = x_1 \oplus (x_0x_3) \oplus (\\
 & x_3x_4) \oplus (x_0x_5) \oplus (x_2x_6) \oplus (x_3x_6) \oplus (x_5x_6) \oplus (x_4x_7) \oplus (x_5x_7) \oplus (x_6x_7) \oplus x_8 \oplus \\
 & (x_0x_8)' \oplus 1'; y_3 = x_0 \oplus (x_1x_2) \oplus (x_0x_3) \oplus (x_2x_4) \oplus x_5 \oplus (x_0x_6) \oplus (x_1x_6) \oplus (\\
 & x_4x_7) \oplus (x_0x_8) \oplus (x_1x_8) \oplus (x_7x_8); y_4 = (x_0x_1) \oplus (x_1x_3) \oplus x_4 \oplus (x_0x_5) \oplus (x_3x_6 \\
 &) \oplus (x_0x_7) \oplus (x_6x_7) \oplus (x_1x_8) \oplus (x_2x_8) \oplus (x_3x_8); y_5 = x_2 \oplus (x_1x_4) \oplus (x_4x_5) \oplus (\\
 & x_0x_6) \oplus (x_1x_6) \oplus (x_3x_7) \oplus (x_4x_7) \oplus (x_6x_7) \oplus (x_5x_8) \oplus (x_6x_8) \oplus (x_7x_8)' \oplus 1'; \\
 y_6 = & x_0 \oplus (x_2x_3) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_4x_5) \oplus (x_3x_6) \oplus (x_4x_6) \oplus (x_5x_6) \oplus x_7 \\
 & \oplus (x_1x_8) \oplus (x_3x_8) \oplus (x_5x_8) \oplus (x_7x_8); y_7 = (x_0x_1) \oplus (x_0x_2) \oplus (x_1x_2) \oplus x_3 \oplus (\\
 & x_0x_3) \oplus (x_2x_3) \oplus (x_4x_5) \oplus (x_2x_6) \oplus (x_3x_6) \oplus (x_2x_7) \oplus (x_5x_7) \oplus x_8' \oplus 1'; y_8 = (\\
 & x_0x_1) \oplus x_2 \oplus (x_1x_2) \oplus (x_3x_4) \oplus (x_1x_5) \oplus (x_2x_5) \oplus (x_1x_6) \oplus (x_4x_6) \oplus x_7 \oplus (\\
 & x_2x_8) \oplus (x_3x_8) \text{ (specification, page 5, line 1, equation 1);}
 \end{aligned}$$

Second equation comprises

$$\begin{aligned}
 y_0 = & (x_1x_3) \oplus x_4 \oplus (x_0x_1x_4) \oplus x_5 \oplus (x_2x_5) \oplus (\\
 & x_3x_4x_5) \oplus x_6 \oplus (x_0x_6) \oplus (x_1x_6) \oplus (x_3x_6) \oplus (x_2x_4x_6) \oplus (x_1x_5x_6) \oplus (x_4x_5x_6); y \\
 1 = & (x_0x_1) \oplus (x_0x_4) \oplus (x_2x_4) \oplus x_5 \oplus (x_1x_2x_5) \oplus (x_0x_3x_5) \oplus x_6 \oplus (x_0x_2x_6) \oplus (\\
 & x_3x_6) \oplus (x_4x_5x_6)' \oplus 1'; y_2 = x_0 \oplus (x_0x_3) \oplus (x_2x_3) \oplus (x_1x_2x_4) \oplus (x_0x_3x_4) \oplus (\\
 & x_1x_5) \oplus (x_0x_2x_5) \oplus (x_0x_6) \oplus (x_0x_1x_6) \oplus (x_2x_6) \oplus (x_4x_6)' \oplus 1'; y_3 = x_1 \oplus (\\
 & x_0x_1x_2) \oplus (x_1x_4) \oplus (x_3x_4) \oplus (x_0x_5) \oplus (x_0x_1x_5) \oplus (x_2x_3x_5) \oplus (x_1x_4x_5) \oplus (x_2x_6
 \end{aligned}$$

$$\begin{aligned} &) \oplus (x_1x_3x_6) ; y_4 = (x_0x_2) \oplus x_3 \oplus (x_1x_3) \oplus (x_1x_4) \oplus (x_0x_1x_4) \oplus (x_2x_3x_4) \oplus (\\ & x_0x_5) \oplus (x_1x_3x_5) \oplus (x_0x_4x_5) \oplus (x_1x_6) \oplus (x_3x_6) \oplus (x_0x_3x_6) \oplus (x_5x_6)' \oplus 1' ; y_5 \\ & = x_2 \oplus (x_0x_2) \oplus (x_0x_3) \oplus (x_1x_2x_3) \oplus (x_0x_2x_4) \oplus (x_0x_5) \oplus (x_2x_5) \oplus (x_4x_5) \oplus (\\ & x_1x_6) \oplus (x_1x_2x_6) \oplus (x_0x_3x_6) \oplus (x_3x_4x_6) \oplus (x_2x_5x_6)' \oplus 1' ; y_6 = (x_1x_2) \oplus (\\ & x_0x_1x_3) \oplus (x_0x_4) \oplus (x_1x_5) \oplus (x_3x_5) \oplus x_6 \oplus (x_0x_1x_6) \oplus (x_2x_3x_6) \oplus (x_1x_4x_6) \oplus (\\ & x_0x_5x_6) \text{ (specification, page 5, line 15, equation 2) ;} \end{aligned}$$

Response to Amendment

20. Applicant has amended claims 1-2, 4-5 and 8 are which necessitated new ground of rejections. See rejection above.

Response to Arguments

21. Applicant's argument filed 28 March 2007, have been fully considered but they are not fully persuasive.

Applicant argues with respect to claim 1 in page 14 that "there is nothing in the alleged combination of AAPA and DKS that discloses or teaches a method for performing a second-round of encryption by encrypting the received the first operated ciphertext bit stream and the second operated ciphertext bit stream having the predetermined time delay with predetermined second encryption codes an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams of length n after once more encrypting the first operated ciphertext bit stream with predetermined second encryption codes,' as recited in claim 1."

Examiner maintains that AAPA discloses performing a second-round of encryption by encrypting the received the first operated ciphertext bit stream (AAPA, specification, page 2, lines 8-10, FOi units. "i" reads on second round, see e.g., FIG. 1, item 220 and FIG. 2B teaches the implementation of item 220, R.sub.4' reads on outputting the third ciphertext bit and L.sub.4' reads on outputting fourth ciphertext bit stream) and the second operated ciphertext bit stream having the predetermined time delay with predetermined encryption codes an odd number of times (FIG. 2B, L.sub.0' reads on first operated ciphertext bit stream and R.sub.0' reads on second operated ciphertext bit stream; FIG. 1 teaches second round (item 220) that takes input from output of first round (item 210) combined with R.sub.0 by performing an exclusive-OR operation which causes time delay), and concurrently outputting the third and fourth ciphertext bit streams of length n after once more encrypting the first operated ciphertext bit stream with predetermined encryption codes (FIG. 2B, specification, page 3, lines 23-30 and page 4, lines 1-15).

Furthermore, using second set of predetermined encryption code for second round encryption is standard in Kasumi encryption algorithm as taught by DKS (page 12, section 4.3, which describes $KO.sub.i = KO.sub.i,1 \parallel KO.sub.i,2 \parallel KO.sub.i,3$ and $Kl.sub.i = Kl.sub.i,1 \parallel Kl.sub.i,2 \parallel Kl.sub.i,3$; "i" represents rounds, see e.g., page 10, section 2.3, line 10).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention

where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, motivation for the rejections is found both in the knowledge generally available to one of ordinary skill in the art and in the cited references.

In response to applicant's argument that AAPA is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, prior art is applicant's discloser. Furthermore, AAPA teaches the first operated ciphertext bit encrypted with predetermined time delay (See AAPA, FIG. 2B, which is an example of an FO unit. Combined with R.sub.0 by performing an exclusive-OR operation, which causes time delay to synchronize two signals).

Applicant argues with respect to claim 5 in page 16 that "there is nothing in AAPA that discloses performing a logical exclusive-OR-operation on the first operated ciphertext bit stream (R.sub.3') and a second encryption code to provide a fourth exclusive-OR-operated bitstream."

Examiner maintains that AAPA discloses generating a second signal by performing a logical exclusive-OR-operation the first operated ciphertext bit stream and the encryption code to provide a fourth exclusive-OR operated bitstream (AAPA,

specification, page 3, lines 20-30, FIG. 2B, which describes a FO.sub.i unit. Where "i" represent number of rounds. Number of exclusive-OR operation depends on number of rounds). Using second set of predetermined encryption code for second round encryption is standard in Kasumi encryption algorithm as taught by DKS (page 12, section 4.3, which describes $KO.sub.i = KO.sub.i,1 \parallel KO.sub.i,2 \parallel KO.sub.i,3$ and $KI.sub.i = KI.sub.i,1 \parallel KI.sub.i,2 \parallel KI.sub.i,3$, "i" reads on 2, see e.g., page 10, section 2.3, line 10). Examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, to increase the confidentiality and integrity of the encrypted data.

Applicant argues with respect to claim 6 in page 18 that "the alleged combination of AAPA, DKS, and Campbell, Jr. doesn't not disclose or teach the claimed elements of claim 6."

Examiner maintains that AAPA teaches AAPA discloses each of the encryptions includes first and second sub-encryptions (FIG. 3, items S91, S71 reads on first sub-encryption and items S92, S72 reads on second sub-encryption). Campbell discloses the outputs are stored and simultaneously retrieved according to an external clock signal (FIG. 1A, column 6, lines 11-16, "the timing signals generated by the control

sequencer 22. The control sequencer 22 controls the sequencing of the various element ...” which describes synchronizing time delay with external clock).

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892.

- US 4,731,843 – Method and device of increasing the execution speed of cipher feedback mode of the DES by an arbitrary multiplier.
- US 5,329,623 – Apparatus for providing cryptographic support in a network.

23. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

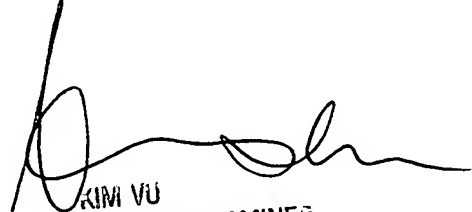
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LD
SD


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100